(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 July 2005 (14.07.2005)

PCT

(10) International Publication Number
WO 2005/062707 A3

(51) International Patent Classification[7]: G06F 11/30, 15/16

(21) International Application Number: PCT/IL2004/001066

(22) International Filing Date: 18 November 2004 (18.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/532,947 30 December 2003 (30.12.2003) US

(71) Applicant *(for all designated States except US)*: CHECK-POINT SOFTWARE TECHNOLOGIES LTD. [IL/IL]; Diamond Tower, 3a Jabotinsky St., 52520 Ramat Gan (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: AHARON, Leeor [IL/IL]; 67 Ahad Ha'am St., 65207 Tel Aviv (IL). COHEN, Cfir [IL/IL]; 8 Haharuv St., 38900 Ceasarea (IL).

(74) Agent: FRIEDMAN, Mark; 7 Jabotinsky St., 52520 Ramat Gan (IL).

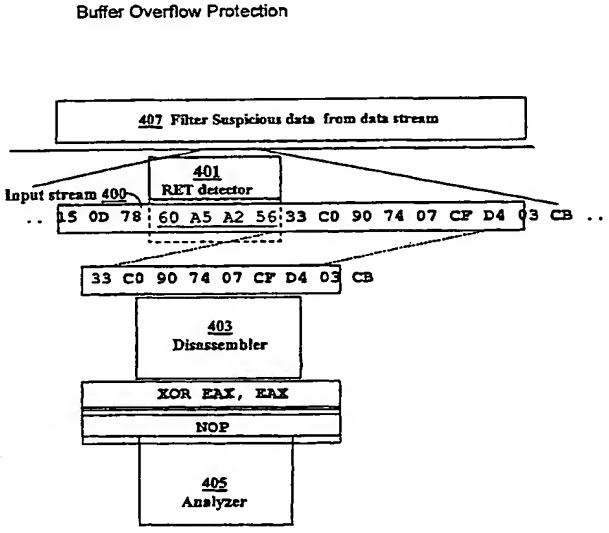
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: UNIVERSAL WORM CATCHER



(57) Abstract: A method for detecting malicious code in a stream of data traffic input (400) to a gateway in a data network by monitoring for suspicious data in the stream of data traffic (407). Upon detecting the suspicious data, an attempt is made to disassemble the suspicious data (403) and a threat weight is assigned for each instruction. The attempt to disassemble is initiated at initial instructions each with a different offset within the suspicious portion of data. The threat weights are accumulated respectively for each branch option in the disassembled code (403), producing respectively an accumulated threat weight for each branch option. When the accumulated threat weight exceeds a previously defined threshold level, an alert is generated and/or traffic is blocked from the source of the malicious code.

WO 2005/062707 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) **Date of publication of the international search report:**
11 August 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.